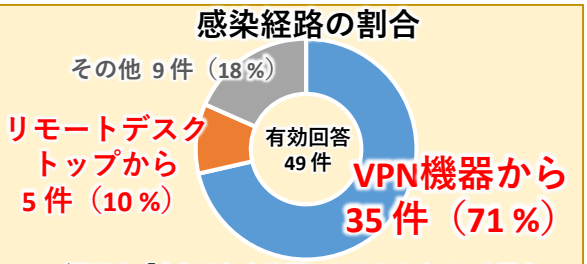
F-CSNET通信かわら版

令和5年11月 号外

⚠テレワーク機器のセキュリティ対策を万全に！⚠

ランサムウェアの感染経路としては、**テレワーク等に利用されるVPN機器のぜい弱性や、強度の弱い認証情報等を利用**して侵入したと考えられるものが大半を占めています。



（警察庁「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」）

実施すべき基本対策はこれ!!

1 ＶＰＮ機器やソフトウェアのアップデート

VPN機器やリモートデスクトップアプリケーション、テレワーク端末のOS等は、最新のアップデートやパッチ適用を実施

2 強力なパスワードの設定

VPN機器やアプリケーション、OS等には、強力なパスワードを設定

3 多要素認証の採用

システムやサービスへの本人認証には、多要素認証方式を採用

4 セキュリティ対策ソフトの利用

テレワーク端末にセキュリティ対策ソフトをインストールし、定義ファイルの自動更新やリアルタイムスキャンを実施

5 オンライン会議ＵＲＬの秘密

オンライン会議にアクセスするためのURLは、正規の参加者以外には非公開にするとともに、会議開催時に、参加予定者以外の人の参加がないかを確認

その他の対策は、総務省が発行している「テレワークセキュリティガイドライン」等を参考に!!（https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/）

◆　福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などを、X（旧Twitter）やホームページに掲載していますので、ぜひご覧ください。

◆　万一、被害に遭われた場合は、管轄警察署あてご一報ください。

【X】旧 Twitter

【HP】